

Title (en)
SIMD INSTRUCTIONS FOR SUPPORTING GENERATION OF HASH VALUES IN CRYPTOGRAPHIC ALGORITHMS

Title (de)
SIMD-BEFEHLE ZUR UNTERSTÜTZUNG DER ERZEUGUNG VON HASH-WERTEN IN KRYPTOGRAPHISCHEN ALGORITHMEN

Title (fr)
INSTRUCTIONS SIMD PERMETTANT DE PRENDRE EN CHARGE LA GÉNÉRATION DE VALEURS DE HACHAGE DANS DES ALGORITHMES CRYPTOGRAPHIQUES

Publication
EP 2742421 A1 20140618 (EN)

Application
EP 12772372 A 20120920

Priority
• GB 201119834 A 20111117
• GB 2012052315 W 20120920

Abstract (en)
[origin: US2013132737A1] A data processing system 2 includes a single instruction multiple data register file 12 and single instruction multiple processing circuitry 14. The single instruction multiple data processing circuitry 14 supports execution of cryptographic processing instructions for performing parts of a hash algorithm. The operands are stored within the single instruction multiple data register file 12. The cryptographic support instructions do not follow normal lane-based processing and generate output operands in which the different portions of the output operand depend upon multiple different elements within the input operand.

IPC 8 full level
G06F 9/30 (2006.01); **G06F 9/38** (2006.01); **H04L 9/08** (2006.01)

CPC (source: EP GB US)
G06F 9/30007 (2013.01 - EP US); **G06F 9/30029** (2013.01 - US); **G06F 9/30032** (2013.01 - US); **G06F 9/30036** (2013.01 - EP GB US); **G06F 9/30145** (2013.01 - US); **G06F 9/3887** (2013.01 - EP GB US); **G06F 9/38873** (2023.08 - EP GB US); **G06F 15/8007** (2013.01 - GB); **G06F 21/602** (2013.01 - US); **G09C 1/00** (2013.01 - EP US); **H04L 9/0643** (2013.01 - EP US); **H04L 9/3236** (2013.01 - GB); **H04L 9/3239** (2013.01 - EP US); **H04L 2209/12** (2013.01 - EP US); **H04L 2209/125** (2013.01 - EP US)

Designated contracting state (EPC)
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

Designated extension state (EPC)
BA ME

DOCDB simple family (publication)
US 2013132737 A1 20130523; US 8966282 B2 20150224; CN 103930869 A 20140716; CN 103930869 B 20171010; EP 2742421 A1 20140618; EP 2742421 B1 20200701; GB 201119834 D0 20111228; GB 2497070 A 20130605; GB 2497070 A8 20130710; GB 2497070 B 20151125; IL 231467 A0 20140430; IL 231467 B 20200331; IN 2111CHN2014 A 20150529; JP 2015501946 A 20150119; JP 6068493 B2 20170125; KR 101962104 B1 20190326; KR 20140093695 A 20140728; MY 168503 A 20181112; TW 201322041 A 20130601; TW I522832 B 20160221; US 2015121036 A1 20150430; US 2016026806 A1 20160128; US 9104400 B2 20150811; US 9703966 B2 20170711; WO 2013072657 A1 20130523

DOCDB simple family (application)
US 201213627209 A 20120926; CN 201280055673 A 20120920; EP 12772372 A 20120920; GB 201119834 A 20111117; GB 2012052315 W 20120920; IL 23146714 A 20140312; IN 2111CHN2014 A 20140319; JP 2014541744 A 20120920; KR 20147014337 A 20120920; MY PI2014700645 A 20120920; TW 101134968 A 20120924; US 201414585900 A 20141230; US 201514792796 A 20150707